0. NULL scan: Hear secrets by pretending not to listen!

`Null scans` send empty TCP packets to a target. Open ports might silently accept them, while closed ports may respond, giving attackers a clue. They're stealthy.

Write a bash script that executes a `TCP NULL` scan on a `host`, targeting ports `20` to `25`.

- Your script should accept `host` as an arguments `$1`.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x06_nmap_advanced_port_scans]
└─⚑  ./0-null_scan.sh www.holbertonschool.com
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-17 15:58 CET
Nmap scan report for www.holbertonschool.com (63.35.51.142)
Host is up (0.078s latency).
Other addresses for www.holbertonschool.com (not scanned): 34.249.200.254
52.17.119.105
rDNS record for 63.35.51.142: ec2-63-35-51-142.eu-west-
1.compute.amazonaws.com

PORT   STATE         SERVICE
20/tcp open|filtered ftp-data
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
24/tcp open|filtered priv-mail
25/tcp open|filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
```